International Journal of Security and Its Applications
Vol.9, No.2 (2015), pp.61-72
http://dx.doi.org/10.14257/ijsia.2015.9.2.07

Selective Encryption Algorithm for GIS Vector Map Using Geometric Objects

Giao Pham Ngoc*, Suk-Hwan Lee** and Ki-Ryong Kwon*$^{\text{Corresponding author}}$

*Dept. of IT Convergence & Application Engineering, Pukyong National University, Pusan, South Korea
Dept. of Information Security, Tongmyong University, Pusan, South Korea
ngocgiaofet@gmail.com, skylee@tu.ac.kr, krkwon@pknu.ac.kr

Abstract

This paper presents the novel selective encryption algorithm for vector map protection for storage, transmission, distribution to authorized users. In proposed algorithm, we just select some values of polylines and polygons in DCT domain to encrypt by random algorithms and cryptography. Experimental results verified that proposed algorithm is effectively and security. Maps are changed whole after encryption process, and unauthorized users cannot access to copy or use them. Encrypted maps do not alter the size of file and not have loss accuracy. The error between original map and decrypted map is approximate zero.

Keywords: *GIS vector map, digital vector map, selective encryption, DCT*

1. Introduction

The vector map, is also called GIS vector map, is a vector-based collection of Geographic Information System (GIS) data about earth at various levels of detail. Vector map is created and developed by the merging system of cartography, statistical analysis, and database technology based on vector model [1-2]. Because vector map has many advantages than raster map, it is used in many domains as research, education, military or digital map services. But the production process of a vector map is considerably complex, and the maintenance of a digital map requires substantial monetary, human resources. Moreover, any companies can buy it, make illegal copies from them or sell them easily many times without taking any permission from the original GIS data provider. In addition, applications of vector map in military require the high security, and must be kept away from unauthorized users. So vector map is necessary to be protected and prevent illegal duplication and distribution of it.

The protection of vector map is to encrypt vector map data, control access of users or identify owner for preventing damages, attacks or illegal distributions which can happen in the integration process of a number of geographical information. Nowadays, to solve that problem, researchers gave watermarking schemes and encryption methods focus on different domains. Looking for the recent security techniques of vector map, the network security techniques for secure transmission or storage and copyright protection of vector map data have been mainly researched. Researchers worked data encryption based on vector map database files or data profile using the cryptography and worked the watermarking of vector map for copyright protection. In fact, the watermarking is only useful for identifying ownership, copyright and prevent illegal distribution while providers desiderate unauthorized users or pirate cannot see and attack to extract the content of vector map in the most cases. Thus, the data encryption is necessary to protect vector map.

ISSN: 1738-9976 IJSIA

Current solutions for vector map data encryption encrypt whole data, thus encryption process has to compute complexity, and spend long time for both encryption and decryption. In addition, data decryption often occur loss data and low accuracy by complex computation on large data. It is not also flexible for various data types. Specially, database management system based security technique is vulnerable by the conversion between data formats. Moreover, current security techniques focus on access of users via internet but the network security technique cannot preserve the security in case of data leakage on off-line or loophole exposure of network administration. So, the security technique for vector map is had to preserve the security in various formats of vector map data, reduce complex computation and encrypted data volume.

For meeting above requirements, in this paper we present a novel selective encryption algorithm for vector map. The main content of proposed algorithm is to transform vertices of polylines, polygon by random algorithms in DCT domain, then select some DC values to encrypt by random values and cryptography. Main advantages of our algorithm are the high efficiency of perceptual encryption by low complexity, adaptive requirement of security and various formats of vector map data. In section 2, we discuss the relation of vector map data to previous algorithms and look into the vector map security techniques. In section 3, we explain the proposed selective encryption algorithm in detail. Then, in section 4 we perform experiments and discuss about the experimental results, evaluate the performance of algorithm. Finally, we conclude this paper in section 5.

2. Related Works

The vector map data is stored in layers. Each layer consists of an amount of vector data which is described as point, polyline and polygon. Point is used to represent simple and zero-dimensional objects while polygon and polyline are used for representing complex and dimensional objects such as road, contour line, railway, lake, boundaries [3]. Therefore, polylines and polygons are considered to be very important components of vector map. And vector map encryption should use them as encrypting targets.

For copyright protection, vector map watermarking has been extensively researched as a solution since the early 2000s. Vector map watermarking schemes are generally focused on geospatial domain methods [4-5] and frequency domain methods [6-7]. The main concept of geospatial watermarking methods is to embed the watermark by modifying the coordinates of vertices while the main concept of watermarking schemes in the frequency domain is to embed the watermark in the spectrum coefficients of DFT, DWT, and DCT transforms of a sequence of vertices or topologies. Summary, the function of vector map watermarking is to verify whether a map is copied or not, it is not the end purpose for security. Therefore, vector map watermarking is not a suitable method to secure vector map for transmission and storage.

In encrypting domain, it has many conventional works relate to management, access, and storage, transmission data [8-13]. Mostly, authors explained technical challenges raised by the unique requirements of secure geospatial data management such as access control, security and privacy policies. But access control and management on Web or database do not maintain security in the outflow of an authenticated user. Relating storage and transmission of vector map, data is encrypted before storing and transmitting. The aim of encryption is to change data by encrypting algorithms using keys, and make unauthorized user cannot access or unable read the content of data. It is also called full encryption. The full encryption process often encrypts all parts of data to change all data. So, selective encryption is necessary to reduce computational complexity, meet storing, transmitting and multimedia applications while achieving a required level of security.

Selective encryption is not a new idea, has been proposed in several applications, especially, in multimedia systems. It is a technique to save computational power, overhead, speed, time. This technique also provides quick security by only encrypting a selected portion of data. Selective encryption technique is one of the most promising solutions to increase the speed of encryption as compared to the full encryption. At this point, various selective encryption techniques for video and image were researched and developed [14] but the selective encryption techniques for vector map data is still poor, and focus network security. Moreover, these methods have several problems about computation complexity and access time. Therefore, in this paper we propose a new selective encryption algorithm for vector map data.

3. The Proposed Algorithm

Vector map data consists of attribute information, display information and geographic information. Both attribute information and display information are stored by text and annotation. The geographic information is geometrical object as polyline and polygon. Thus, we defined general processing of the proposed algorithm for vector map as Figure 1. In vector encryption block, text and annotation are not encrypted while polylines and polygons are performed selective encryption. To simple notation, we consider polyline and polygon as an object with a series of vertices which polyline and polygon are denoted as the same object.

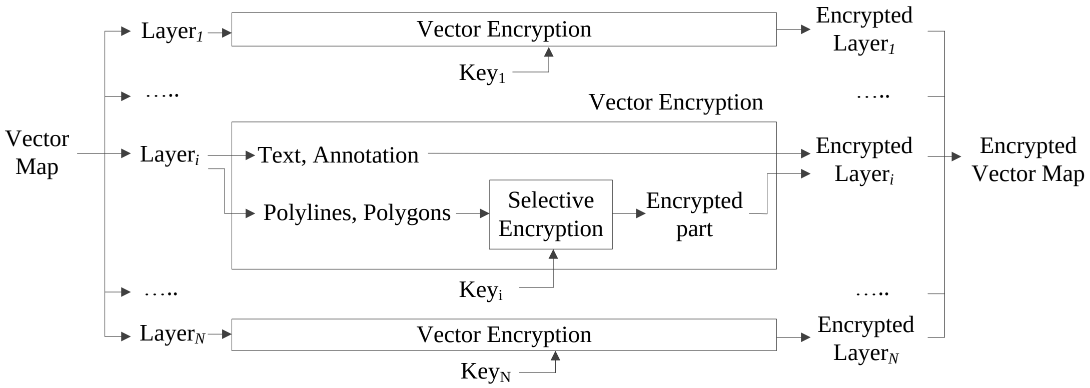


Figure 1. General Processing of the Proposed Algorithm for Vector Map

3.1. Selective Encryption

Because, each object is a set of series vertices, thus we consider each object as a 1D vector. Objects in a layer $\mathbf{L}_i$ are classified into G groups to identify them before vertices randomization. The purpose of clustering process is to identify objects by groups and after 1D-DCT processing all DC values in each group are encrypted by corresponding random value. It helps us no must generate and use many random values for DC values encryption because the total number of DC values in each layer is different. Moreover, it is also flexible and high security because the number of groups and clustering algorithm are defined and chosen by user. The selective encryption and decryption are described in the Figure 2.

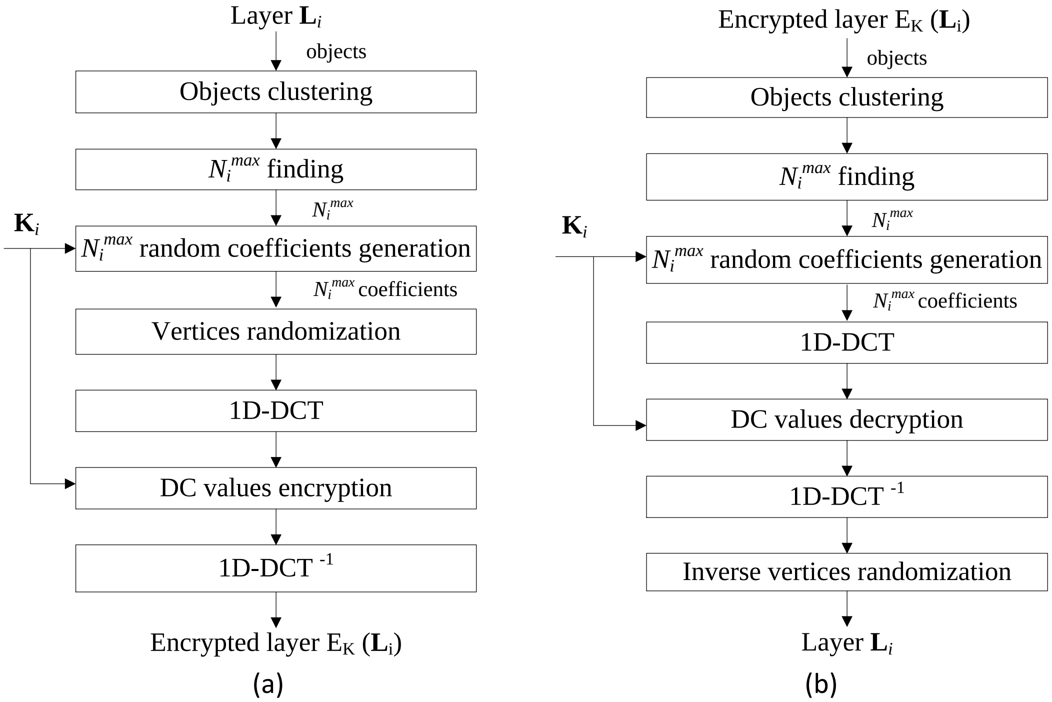


Figure 2. The Proposed Algorithm; (a) Selective Encryption, (b) Selective Decryption

Each layer has many objects; the total number of objects in each layer is different. Thus, if each DC value of each object in DCT domain is encrypted by a random value, we must generate random values so much, and it is easy to detect and decrypt because this information is stored by text. Therefore, objects are necessary to be classified. In order to divide objects into groups, we use K-means algorithms based on properties of objects. Objects have properties number of parts, number of points and the value of vertices but in vertices randomization and DCT domain, value of vertices is changed. Thus, we only use properties as number of parts, number of points to classify them into G groups, and K-means algorithm is fitted in this case.

The purpose of N_i^{max} finding is to generate random vector $\mathbf{r}_i$ has N_i^{max} random coefficients. The N_i^{max} is maximum number of vertices of an object among objects in a layer $\mathbf{L}_i$:

$$N_i^{max} = max_{j\in[1,N_i]} N_{ij} \quad (1)$$

The key $\mathbf{K}_i$ is used as seed of pseudo-random function $R_K(\,)$ to create N_i^{max} random coefficients of random vector $\mathbf{r}_i$ and encrypt DC values in DCT coefficients. It is generated randomly by SHA-512 algorithm from user key with key length is 512 bit for each key [15]. The Figure 3 shows a random key process for random coefficients generation and DCT coefficients encryption.

The random vector $\mathbf{r}_i = \{r_{ik} | k \in [1, N_i^{max}]\}$ is used to randomize vertices of objects. The value r_{ik} is calculated by pseudo-random function $R_K(\,)$ using $\mathbf{K}_i$ as equation (2):

$$r_{ik} = k \times R_K(\mathbf{K}_i) | k \in [1, N_i^{max}] \quad (2)$$

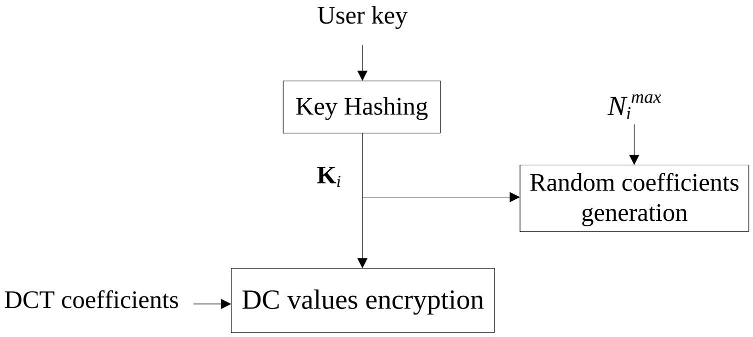


Figure 3. A Random Key Process for Random Coefficients Generation & DCT Coefficients Encryption

In vertices randomization step, we randomize vertices in an object by randomized function $R_V(\,)$ using random coefficients of random vector $\mathbf{r}_i$ varying the number of vertices in that object as equation (3):

$$\mathbf{P}'_{ij} = R_V(\mathbf{P}_{ij}, \mathbf{r}_i) = \{v_{ij,k} \times r_{ik} | k \in [1, N_{ij}]\} \tag{3}$$

After vertices randomization, we apply 1D-DCT for randomized objects to get DCT coefficients of objects $\mathbf{P}_{ij}$ is $\mathbf{F}_{ij} = \{(u_{ij,k}, v_{ij,k}) | k \in [1, N_{ij}]\}$. In DCT domain, we encrypt selectivity DC values by random values using $\mathbf{K}_i$. To do that work, we firstly create $\mathbf{r}_G = \{r_g | g \in [1, G]\}$ is a set includes G random values corresponding to G groups of objects, using $\mathbf{K}_i$ as equation (4):

$$r_g = g \times R_K(\mathbf{K}_i) | g \in [1, G] \tag{4}$$

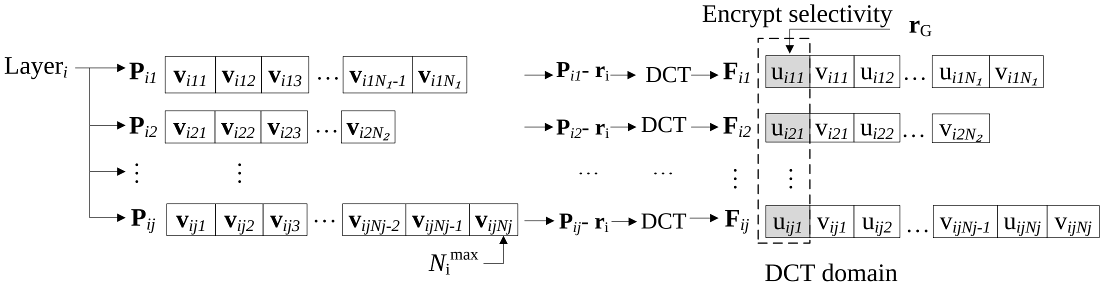

Encrypt selectivity
$\mathbf{r}_G$
Layer$_i$
$\mathbf{P}_{i1}$ $\mathbf{v}_{i11}$ $\mathbf{v}_{i12}$ $\mathbf{v}_{i13}$ … $\mathbf{v}_{i1N_1\text{-}1}$ $\mathbf{v}_{i1N_1}$
$\mathbf{P}_{i2}$ $\mathbf{v}_{i21}$ $\mathbf{v}_{i22}$ $\mathbf{v}_{i23}$ … $\mathbf{v}_{i2N_2}$
$\mathbf{P}_{ij}$ $\mathbf{v}_{ij1}$ $\mathbf{v}_{ij2}$ $\mathbf{v}_{ij3}$ … $\mathbf{v}_{ijNj\text{-}2}$ $\mathbf{v}_{ijNj\text{-}1}$ $\mathbf{v}_{ijNj}$
$N_\mathrm{i}^{\mathrm{max}}$
$\mathbf{P}_{i1}$- $\mathbf{r}_\mathrm{i}$ DCT $\mathbf{F}_{i1}$
$\mathbf{P}_{i2}$- $\mathbf{r}_\mathrm{i}$ DCT $\mathbf{F}_{i2}$
$\mathbf{P}_{ij}$- $\mathbf{r}_\mathrm{i}$ DCT $\mathbf{F}_{ij}$
u_{i11} v_{i11} u_{i12} … u_{i1N_1} v_{i1N_1}
u_{i21} v_{i21} u_{i22} … v_{i2N_2}
u_{ij1} v_{ij1} u_{ij2} … $\mathrm{v}_{ijNj\text{-}1}$ u_{ijNj} v_{ijNj}
DCT domain

Figure 4. Selective Encryption Process of the Proposed Algorithm

Secondly, we multiple DC value of object with a random value in $\mathbf{r}_G$ to get encrypted DCT coefficients of $\mathbf{P}_{ij}$ as equation (5). This random value is corresponding value to classified group of object above. Selective encryption process of the proposed algorithm is described in the Figure 4.

$$E_K(\mathbf{F}_{ij}) = \{(u_{ij,1} \times r_g, v_{ij,1}), (u_{ij,2}, v_{ij,2}), \dots, (u_{ij,N_{ij}}, v_{ij,N_{ij}})\} \tag{5}$$

Finally, we get recovered object from $E_K(\mathbf{F}_{ij})$ by inverse 1D-DCT is $E_K(\mathbf{P}_{ij}) = \{e_{ij,k} | k \in [1, N_{ij}]\}$. This is selectivity encrypted object. And encrypted layer is a set of encrypted objects $E_K(\mathbf{L}_i) = \{E_K(\mathbf{P}_{ij}) | j \in [1, N_i]\}$.

3.2. Selective Decryption

Selective decryption is the inverse process with selective encryption. Following Figure 2.b, steps in selective decryption such as objects clustering, N_i^{max} finding, random coefficients generation and DCT are computed similar steps and equations in selective encryption, except DC values decryption and inverse vertices randomization step. So, in this section we just discuss DC values decryption and inverse vertices randomization.

Following steps in selective decryption in Figure 2.b, after 1D-DCT process we receive encrypted DCT coefficients of object $E_K(\mathbf{F}_{ij})$. Refer to equation (5), in DC values decryption we only need to divide DC value for r_g as following corresponding group of classified object to get $\mathbf{F}_{ij}$. After 1D-DCT^{-1} we get randomized object $\mathbf{P'}_{ij}$, decrypted object $\mathbf{P}_{ij}$ is recovered by inverse vertices randomization using random vector $\mathbf{r}_i$ varying the total number of vertices in an object using equation (6):

$$\mathbf{P}_{ij} = R_V^{-1}(\mathbf{P'}_{ij}, \mathbf{r}_i) = \{v'_{ij,k} \div r_{ik} | k \in [1, N_{ij}]\} \quad (6)$$

4. Experiment and Algorithm Evaluation

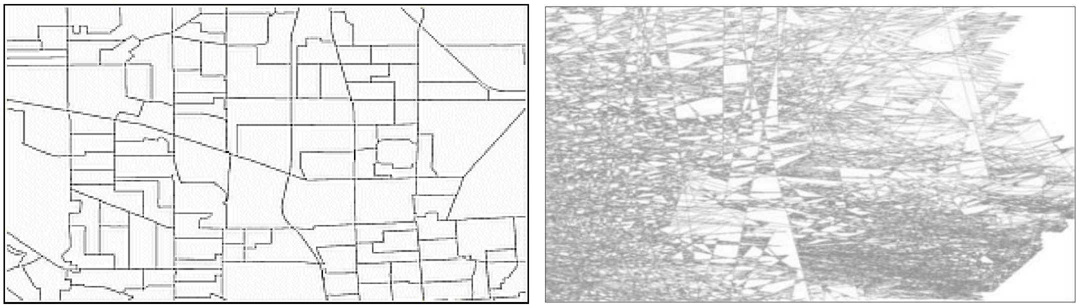
In this paper, we proposed the novel selective encryption algorithm in DCT domain for vector map security. We used scaling maps as Table.1 in visualization experiences. In comparison with conventional works, the proposed algorithm responses the security in various formats of vector map data, reduces complex computation and encrypted data volume, responses multimedia applications. Comparing to previous solutions, the proposed algorithm has high security because they manipulated on vector map data, not manage access control via data management systems. The proposed algorithm also meets the requirement of security by the length of keys.

Table 1. Scaling Maps in Experiments

Test Map	Scale	Number of layers	Number of objects
LA 1	1:5000	1	103
LA 2	1:10000	2	294
LA 3	1:100000	3	7191
LA 4	1:250000	5	79255
LA 5	1:500000	7	445651

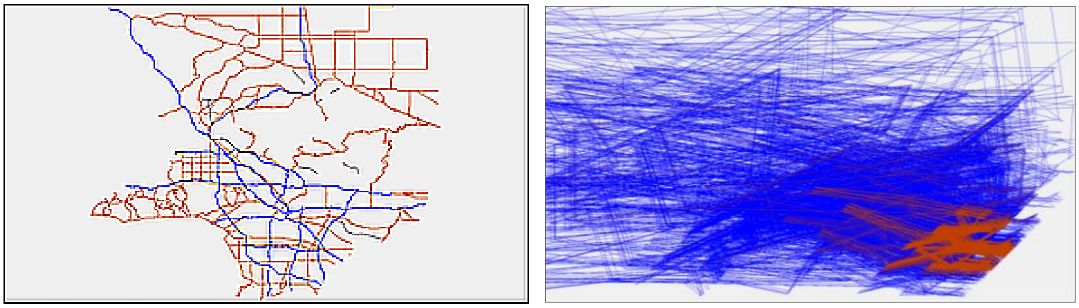
4.1. Visualization

Experimental results from Figure 5 to Figure 9 show the proposed algorithm changes whole maps. The proposed algorithm has much lower computational complexity than AES or DES because we select only DC value in DCT domain and encrypt it by random value. But we confirmed it effectively by experimental results which are showed from Figure 5 to Figure 9. Moreover, our selective encryption process changes only values of vertices in polylines and polygons of map. It did not alter the size of encrypted file, so do not have loss data happen. We also show original maps beside encrypted maps by proposed method to compare differences between themselves and original maps.



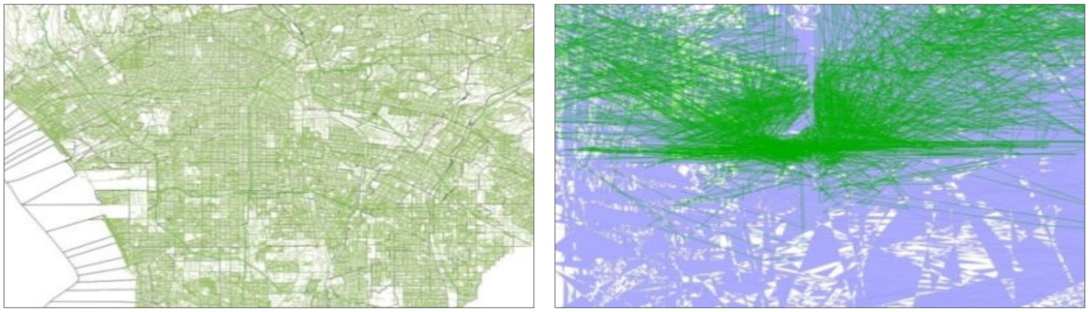
(a) (b)

Figure 5. Experimental Result with LA1; (a) Original Map, (b) Encrypted Map



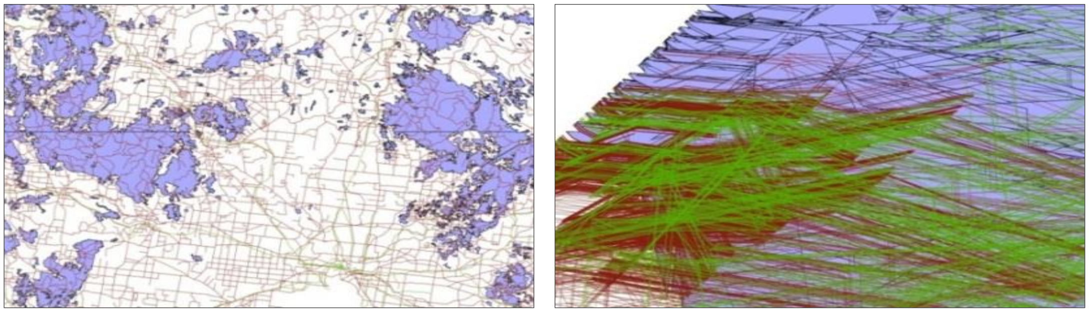
(a) (b)

Figure 6. Experimental Result with LA2; (a) Original Map, (b) Encrypted Map



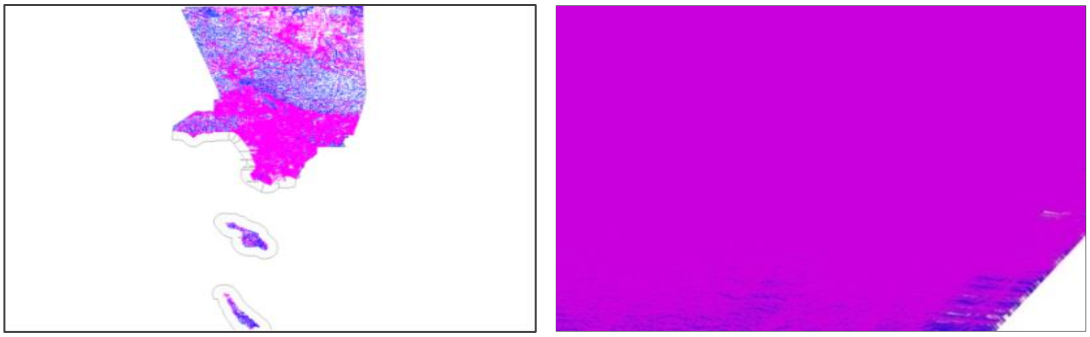
(a) (b)

Figure 7. Experimental Result with LA3; (a) Original Map, (b) Encrypted Map



(a) (b)

Figure 8. Experimental Result with LA4; (a) Original Map, (b) Encrypted Map



(a) (b)

Figure 9. Experimental Result LA5; (a) Original Map, (b) Encrypted Map

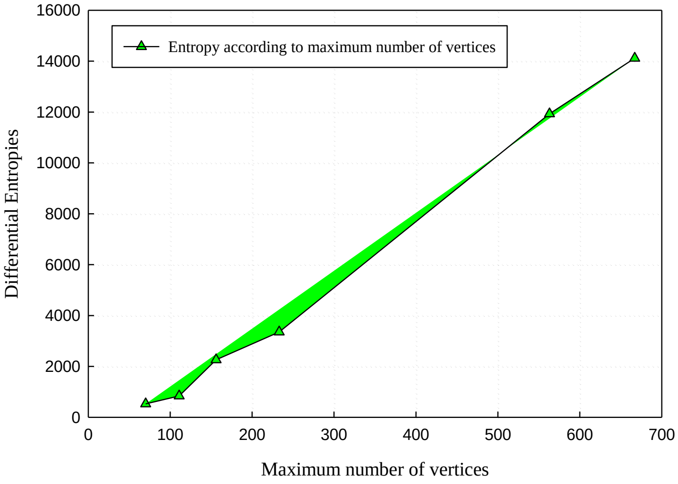
4.2. Security Evaluation

In proposed algorithm, $\mathbf{r}_i$ is a set of random values $r_{ik},\ k \in [1, N_i^{max}]$ therein r_{ik} is random value on sample space S_r has Ω_r elements. Similarly, we also have $\mathbf{r}_G$ is a set of random values $r_g,\ g \in [1, G]$ therein r_g is random value on sample space S_G has Ω_G elements. These random values are independent random variables. Therefore, entropy of the proposed algorithm h_D is depended on two random values r_{ik}, r_g:

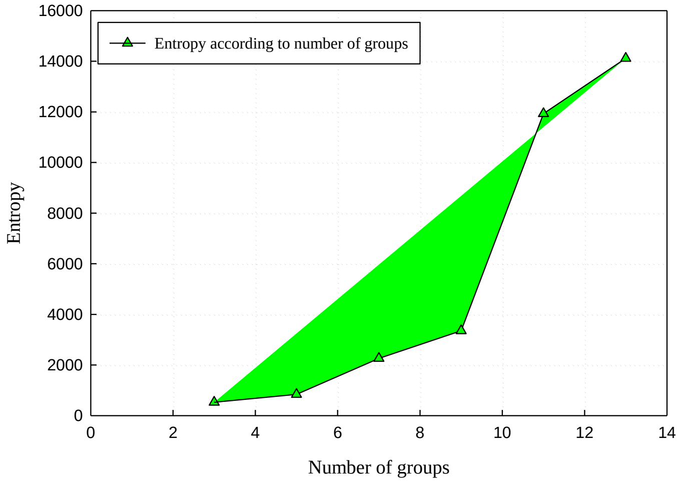
$$h_D = \sum_{k=1}^{N_i^{max}} h(r_{ik}) + \sum_{g=1}^{G} h(r_g) \tag{7}$$

With $h(r_{ik}),\ h(r_g)$ are corresponding entropies of random values r_{ik}, r_g. In our experiment, we used pseudo-random function $R_K(\,)$ with discrete uniform distribution, thus equation (7) becomes equation (8), and h_D is determined by $N_i^{max}, G, \Omega_r, \Omega_G$.

$$h_D = N_i^{max}.\,ln(\Omega_r) + G.\,ln(\Omega_G) \tag{8}$$



(a)



(b)

Figure 10. Entropy of the Proposed Algorithm; (a) According to Maximum Number of Vertices, (b) According to Number of Groups

Moreover, we used SHA-512 algorithm with 128 bits salt to generate random keys. Thus, if user uses one of L_k English words as his password, an attacker has to calculate $L_k \times 2^{128}$ keys to access encrypted data, each key length is 512 bits.

4.3. Uniqueness Evaluation

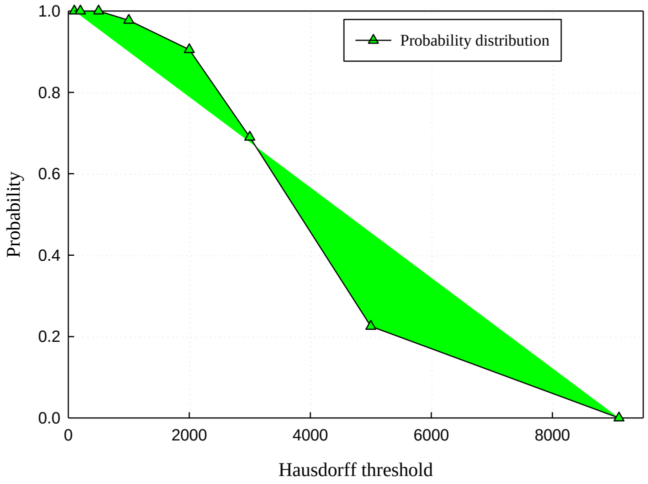


Figure 11. Probability Distribution According to Pre-defined Hausdorff Distance Threshold

Assume that $E'_K(\mathbf{L}_i)$ and $E''_K(\mathbf{L}_i)$ are corresponding encrypted map by $\mathbf{K}'_i \neq \mathbf{K}''_i$, we measured the normalized Hausdorff distances $d_H(E'_K, E''_K)$ between $E'_K(\mathbf{L}_i)$ and $E''_K(\mathbf{L}_i)$ from 1000 different keys and analyzed probability with pre-defined Hausdorff distance threshold. We gave differential thresholds to compute probability distribution as Figure 11. Accordingly, in the range [0, 10000], Pr $[d_H(E'_K, E''_K) > Th] = 1$ with $Th \in [0,\ 500]$, equal 0.977 with $Th = 1000$ and decreases to 0 when $Th = 9100$. Here, Pr is the probability and Th is pre-defined Hausdorff distance threshold.

5. Conclusion

My paper focuses on the issues how to encrypt GIS vector map selectivity with low complexity. Experimental results showed that the proposed algorithm has very effective with a large volume of GIS dataset. Decrypting results also show the error in decryption process approximates zero. In comparison with previous algorithm, our algorithm has very low complex computation, while it responses requires of security. The proposed algorithm can be applied to various file formats or standard vector map, and can be used for map database security of GIS map service on on/off-lines. Furthermore, my algorithm can be applied to various vector contents such as CAD and 3D content fields.

Acknowledgement

This work was supported by a Research Grant of Pukyong National University (2014Year).

References

[1] K. E. Foote and M. Lynch, “Geographic Information Systems as an Integrating Technology: Context, Concepts, and Definitions”, (**2009**).

[2] M. F. Goodchild, “Twenty years of progress: GIS science in 2010”, Journal of Spatial Information Science, no. 1, (**2010**), pp. 3-20.

[3] An ESRI White Paper: ESRI Shape-file Technical Description. Environmental Systems Research Institute, USA, (**1998**).

[4] C. Wang, and Z. Peng, Y. Peng, L. Yu, J. Wang and Q. Zhao, “Watermarking geographical data on spatial topological relations”, Proceeding of Multimedia Tools and Applications, (**2012**) March.

[5] S.-H. Lee and K.-R. Kwon, “Vector Watermarking Scheme for GIS Vector Map Management”, Multimedia Tools and Applications, published online (**2011**).

[6] R. Ohbuchi, H. Ueda and S. Endoh, “Watermarking 2D vector maps in the mesh-spectral domain”, Proceeding of International Conference on Shape Modeling and Applications, (**2003**) May.

[7] V. Solachidis and I. Pitas, “Watermarking polygonal lines using Fourier descriptors”, IEEE Computer Graphics and Applications, vol. 24, no. 3, (**2004**), pp. 44–51.

[8] G. Li, “Research of Key Technologies on Encrypting Vector Spatial Data in Oracle Spatial”, Proceeding of International Conference on Industrial Electronics and Computer Science, (**2010**) December.

[9] E. Bertino and M. L. Damiani, “A Controlled Access to Spatial Data on Web”, Proceeding of Conference on Geographic Information Science, (**2004**) April.

[10] S.-C. Chena, X. Wangb, N. Rishea and M. A. Weiss, “A web-based spatial data access system using semantic R-trees”, Journal of Information Sciences, vol. 167, (**2003**), pp. 41-61.

[11] F. Wu, W. Cui and H. Chen, “A Compound Chaos-Based Encryption Algorithm for Vector Geographic Data under Network Circumstance”, Proceeding of Cardholder Information Security Program, (**2008**) May.

[12] Y. Dakroury, I. A. El-ghafar and A. Tammam, “Protecting GIS Data Using Cryptography and Digital Watermarking”, International Journal of Computer Science and Network Security, vol. 10, no. 1, (**2010**), pp. 75-84.

[13] B. Jang, S. Lee and K. Kwon, “Perceptual encryption with compression for secure vector map data processing”, Journal Digital Signal Processing, vol. 25, (**2014**), pp. 224-243.

[14] A. Massoudi, F. Lefebvre, C. De Vleeschouwer, B. Macq and J.-J.Quisquater, “Overview on Selective Encryption of Image and Video: Challenges and Perspectives”, Hindawi Publishing Corporation EURASIP Journal on Information Security, no. 5 (**2008**).

[15] RSA Laboratories, PKCS #5 v2.1: Password-Based Cryptography Standard, (**2006**) October.

Authors

Giao Pham Ngoc, He received B.E degree in School of Electronic & Telecommunication in Hanoi University of Science & Technology (HUST) in 2011, and Master degree from Pukyong National University (PKNU), Busan, South Korea in 2014. Currently, he is a researcher in Multimedia Communication & Signal Processing Lab in PKNU. His research interests include video processing & application, GIS applications, data security and smart system.

Suk-Hwan Lee, He received the B.S., M.S., and Ph.D. degrees in Electrical Engineering from Kyungpook National University, Korea in 1999, 2001, and 2004 respectively. He is currently an associate professor in Department of Information Security at Tongmyong University and a member of executive committee of IEEE R10 Changwon Section. His research interests include multimedia security, digital image processing, and computer graphics.

Ki-Ryong Kwon, He received the B.S., M.S., and Ph.D. degrees in electronics engineering from Kyungpook National University in 1986, 1990, and 1994 respectively. He worked at Hyundai Motor Company from 1986-1988 and at Pusan University of Foreign Language from 1996-2006. He is currently a professor in Department of IT Convertgence and Application Engineering at the Pukyong National University. He has researched University of Minnesota in USA on 2000~2002 with Post-Doc, and Colorado State University on 2011~2012 with visiting professor. He is currently the General Affair Vice President of Korea Multimedia Society. His research interests are in the area of digital image processing, multimedia security and watermarking, bioinformatics, weather radar information processing.